AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, said data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to said first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to said first bus;

a second bus;

a first interface circuit interposed between said first bus and said second bus;

an encryption processing circuit connected to said second bus, for decrypting the content key data;

a public key encryption module that performs authentication, creates signature data, encrypts and decrypts data for transferring, and shares a session key data obtained by the authentication;

a common key encryption module that performs mutual authentication and encrypts and decrypts data by using the session key data;

an external bus interface circuit connected to said second bus; and

a usage monitor;

wherein said arithmetic processing circuit determines at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data, and creates log data which includes a unique identifier of the content data, discount information, and tracing information and indicates result of the determined mode; and the arithmetic processing circuit creates usage control status data in accordance with the determined purchase mode, and controls the use of the content data based on the usage control status data;

said usage control status data comprising a content identification for said content data, the purchase mode, an identification for said tamper-resistant circuit module, and a user identification for a user who has purchased said content data;

wherein the usage monitor monitors said usage control policy data and said usage control status data to make sure that said content data is purchased and used as restricted by said usage control policy data and said usage control status data; and

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.

2. (Original) A data processing apparatus according to claim 1, further comprising a second interface circuit within said tamper-resistant circuit module, wherein said first bus comprises a third bus connected to said arithmetic processing circuit and said storage circuit, and a fourth bus connected to said first interface circuit, and said second interface circuit is interposed between said third bus and said fourth bus.

3. (Original) A data processing apparatus according to claim 2, further comprising within said tamper-resistant circuit module:

a fifth bus;

a third interface circuit connected to said fifth bus, for performing communication with a data processing circuit having an authentication function which is loaded on one of a recording medium and an integrated circuit card; and

a fourth interface circuit interposed between said fourth bus and said fifth bus.

4. (Original) A data processing apparatus according to claim 1, wherein said encryption processing circuit comprises a public-key encryption circuit and a common-key encryption circuit.

5. (Previously Presented) A data processing apparatus according to claim 4, wherein:

said storage circuit stores private key data of said data processing apparatus and public key data of a second data processing apparatus;

said public-key encryption circuit verifies the integrity of signature data, which verifies the integrity of the content data, the content key data, and the usage control policy data, by using the public key data, and when recording the content data, the content key data, and the usage control policy data on a recording medium or when sending the content data, the content key data, and the usage control policy data to said second data processing apparatus, said public-key encryption circuit creates signature

data, which verifies the integrity of the content data, the content key data, and the usage control policy data, by using the private key data; and

said common-key encryption circuit decrypts the content key data, and when sending the content data, the content key data, and the usage control policy data to said second data processing apparatus online, said common-key encryption circuit encrypts and decrypts the content data, the content key data, and the usage control policy data by using session key data obtained by performing mutual authentication with said second data processing apparatus.

6. (Original) A data processing apparatus according to claim *5,* further comprising a hash-value generating circuit within said tamper-resistant circuit module, for generating hash values of the content data, the content key data and the usage control policy data, wherein said public-key encryption circuit verifies the integrity of the signature data and creates the signature data by using the hash values.

7. (Previously Presented) A data processing apparatus according to claim 1, further comprising a random-number generating circuit within said tamper-resistant circuit module, said random-number generating circuit being connected to said second bus, for generating a random number for performing mutual authentication with a second data processing apparatus when sending the content data, the content key data, and the usage control policy data to said second data processing apparatus online.

8. (Original) A data processing apparatus according to claim 1, wherein said external bus interface circuit is connected to an external storage circuit for storing at least one of the content data, the content key data, and the usage control policy data.

9. (Original) A data processing apparatus according to claim 8, further comprising a storage-circuit control circuit for controlling access to said storage circuit and access to said external storage circuit via said external bus interface circuit in accordance with a command from said arithmetic processing circuit.

10. (Original) A data processing apparatus according to claim 1, wherein said external bus interface circuit is connected to a host arithmetic processing apparatus on which said data processing apparatus is loaded.

11. (Original) A data processing apparatus according to claim 8, further comprising a storage management circuit for managing an address space of said storage circuit and an address space of said external storage circuit.

12-14. (Canceled)

15. (Original) A data processing apparatus according to claim 4, wherein, when the content key data is encrypted with license key data having an effective period, said storage circuit stores the license key data, said data processing apparatus further comprises a real time clock for generating real time, said arithmetic processing circuit

reads the effective license key data from said storage circuit based on the real time indicated by said real time clock, and said common-key encryption circuit decrypts the content key data by using the read license key data.

16. (Original) A data processing apparatus according to claim 1, wherein said storage circuit writes and erases data in units of blocks, and said data processing apparatus comprises within said tamper-resistant circuit module, a write-lock control circuit for controlling the writing and erasing of the data into and from said storage circuit in units of blocks under the control of said arithmetic processing circuit.

17. (Currently Amended) A data processing apparatus for performing rights processing of content data encrypted with content key data based on usage control policy data, and for decrypting the encrypted content key data, said data processing apparatus comprising within a tamper-resistant circuit module:

a first bus;

an arithmetic processing circuit connected to said first bus, for performing the rights processing of the content data based on the usage control policy data;

a storage circuit connected to said first bus;

a second bus;

an interface circuit interposed between said first bus and said second bus;

an encryption processing circuit connected to said second bus, for decrypting the content key data;

a public key encryption module that performs authentication, creates signature data, encrypts and decrypts data for transferring, and shares a session key data obtained by the authentication;

a common key encryption module that performs mutual authentication and encrypts and decrypts data by using the session key data

an external bus interface circuit connected to said second bus; and

a usage monitor;

wherein, upon receiving an interrupt from an external circuit via said external bus interface circuit, said arithmetic processing circuit becomes a slave for said external circuit so as to perform processing designated by the interrupt, and reports a result of the processing to said external circuit;

wherein said arithmetic processing circuit determines at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data, and creates log data which includes a unique identifier of the content data, discount information, and tracing information and indicates a result of the determined mode; and the arithmetic processing circuit creates usage control status data in accordance with the determined purchase mode, and controls the use of the content data based on the usage control status data;

said usage control status data comprising a content identification for said content data, the purchase mode, an identification for said tamper-resistant circuit module, and a user identification for a user who has purchased said content data;

wherein the usage monitor monitors said usage control policy data and said usage control status data to make sure that said content data is purchased and used as restricted by said usage control policy data and said usage control status data; and

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.

18. (Original) A data processing apparatus according to claim 17, wherein said arithmetic processing circuit reports the result of the processing by outputting an interrupt to said external circuit.

19. (Original) A data processing apparatus according to claim 17, wherein said external bus interface comprises a common memory for said arithmetic processing circuit and said external circuit, and said arithmetic processing circuit writes the result of the processing into said common memory, and said external circuit obtains the result of the processing by polling.

20. (Original) A data processing apparatus according to claim 19, wherein said external bus interface comprises:

a first status register indicating an execution status of the processing requested from said external circuit in said arithmetic processing circuit, and including a flag set by said arithmetic processing circuit and read by said external circuit;

a second status register indicating whether said external circuit has requested said arithmetic processing circuit to perform processing, and including a flag set by said external circuit and read by said arithmetic processing circuit; and

said common memory for storing a result of the processing.

21. (Original) A data processing apparatus according to claim 18, wherein said storage circuit stores an interrupt program describing the processing designated by the interrupt, and said arithmetic processing circuit performs the processing by executing the interrupt program read from said storage circuit.

22. (Original) A data processing apparatus according to claim 21, wherein said storage circuit stores a plurality of said interrupt programs, and a plurality of sub-routines to be read when executing the interrupt program, and said arithmetic processing circuit appropriately reads and executes the sub-routines from said storage circuit when executing the interrupt program read from said storage circuit.

23-56. (Canceled)

57. (Currently Amended) A data processing method of performing rights processing for content data encrypted with content key data based on usage control policy data, and of decrypting the encrypted content key data, said data processing method comprising the steps of:

determining at least one of a purchase mode and a usage mode of the content data based on a handling policy indicated by the usage control policy data;

creating log data which includes a unique identifier of the content data, discount information, and tracing information and indicates a result of the determined purchase mode;

creating usage control status data in accordance with the determined purchase mode; said usage control status data comprising a content identification for said content data, the purchase mode, an identification for a tamper-resistant circuit module, and a user identification for a user who has purchased said content data;

monitoring said usage control policy data and said usage control status data to make sure that said content data is purchased and used as restricted by said usage control policy data and said usage control status data;

controlling the use of the content data based on the usage control status data;

recording the content data, for which the purchase mode is determined, on a recording medium; and

performing authentication;

creating a signature data;

sharing session key data obtained by the authentication;

encrypting the content key data and the usage control status data by using the session key data ~~medium key data corresponding to said recording medium~~;

wherein the purchase mode is determined from one or more purchase mode options, and each purchase mode option has a different level of restriction imposed on a playback operation.